IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 18, Issue 1, Ver. III (Jan – Feb. 2016), PP 104-114
www.iosrjournals.org

Threats and Security using Trust Techniques in Wireless Sensor Networks

Vaishali Gupta[1], Manik Gupta[2]
[1]*(Department of Computer Science and Engineering, Chitkara University, India)*
[2]*(Department of Computer Science and Engineering, Chitkara University, India)*

Abstract: *Wireless Sensor Networks are implementing on large scale in real time environments due to its incredible uses in real life. Wireless Sensor Networks don't need human interference for its working so they can place where human cannot reach easily. As sensor nodes are placed in an open and insecure environment, they are prone to security attacks by adversaries. So, the security is an important issue in sensor networks. Traditional security mechanisms like cryptography, intruder detection, routing protocols were implemented to provide security in wireless sensor networks. These mechanisms are capable to detect and remove internal attacks but fail to detect compromised nodes in a network. Compromised node exposes all secrets of network to the adversary which in turn put all existing mechanisms at risk. To overcome this problem various trust and reputation mechanisms have been proposed. Trust can be calculated in two ways. First, it can directly calculate with the past behavior of nodes. Secondly, it can be indirectly combined with the reputation of a node from the recommenders. Recommenders are neighbors of a node. In this paper, various security threats to the network, traditional security techniques, and various reputation and trust mechanisms have been discussed.*

Keyword: *Wireless Sensor Networks, Sensor Node, Network Attacks, Security Mechanisms, Reputation, Trust.*

I. Introduction

Wireless sensor network is a combination of wireless connected devices which can communicate in an open environment, senses data, and monitors the physical information in the real time environment. This type of networks do not need human interference for communication purposes, they do their work without human beings and send the information on their own. They are beneficial in those types of environments and areas in which humans are unable to access. The sensor nodes are distributed randomly on large area according to the need of the particular application. [1, 2, 3]

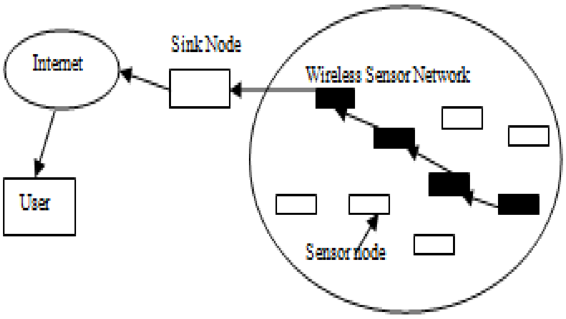


Fig. 1. General Structure of Wireless Sensor Network

1.1 Sensor Nodes

Wireless sensor network is a combination of tiny sensor nodes which are used to sense the physical data and later can convert it into the digital signals. Sensor nodes can also called as Motes. They can be small or large in size. Sensor nodes are designed according to the environment in which they have to place and application on which they have to work. Sensor nodes are different for different applications and environment. Sensor nodes consist of micro-controller which is used to control the monitoring of node, a radio transceiver for generating radio waves, antenna, sensing unit, battery etc. These sensor nodes communicate with each other via radio interface. Nodes have limited number of capacity for storing the data and battery consumption. [2, 3]

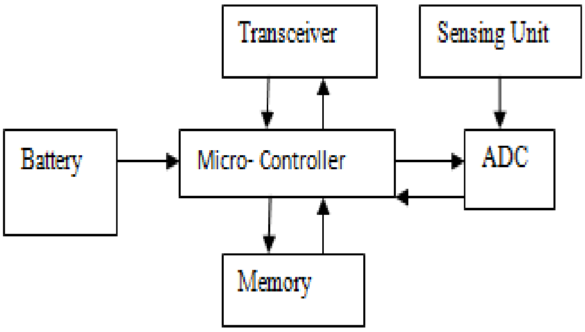


Fig. 2. Architecture of Sensor Node

II. Applications

2.1 Military Applications

Security is the main purpose for Military. Tasks like information gathering, tracking enemies, observing battlefield wireless sensor networks play an important role for this. The project "A line in the sand" has been developed by Ohio State University which justifies this application. This project involves deployment of ninety nodes which are capable to detect metallic objects. The aim to develop this project was, it can detect moving objects with the metallic content and armed soldiers. The sensor nodes can be placed at the Line of Control to detect the presence of enemies. [4]

2.2 Environmental Monitoring

2.2.1 Indoor Environmental Monitoring:

Indoor monitoring uses match box size sensor nodes for monitoring light, temperature, frames' status (windows, doors), air streams and indoor air pollution. This is used to control indoor environment. It can also be used in fire and smoke detection. Sensor networks may also be useful after an earthquake. The inspection of a building after an earthquake provides the real data. [5]

2.2.2 Outdoor Monitoring (Habitat Monitoring)

There is a potential impact of human presence in the habitats for monitoring plants and animals. The human disturbance can reduce breeding rate or can even destroy sensitive population by increasing stress of their presence. Deployment of sensor networks can overcome this situation. Sensor nodes can be deployed in the breeding season or other sensitive period. [6, 7]

2.3 Health Care Applications

In the health sciences and the health care system wireless sensors are very effective. Alzheimer, which is a cognitive disorder can be monitored and controlled by wireless sensors at its early stages. [8]

2.4 Applications to Robotics

Robotics is a vast subject. The combination of sensor nodes (motes) and robots leads to the development of new applications. The USC centre developed a tiny robot named Robomote for robotics and embedded systems to promote research in large scale sensor networks. Robots participate to perform tasks. [9, 10]

III. Network Attacks

Unlike other networks, wireless sensor networks are very much prone to physical attacks in the real time environments. Anyone can sense data; sensor nodes can be destroyed or can be monitored by the attacker. The sensor nodes can be tampered or can be physically replaced by the malicious nodes. Therefore, the physical security in sensor networks is very important. Wireless Sensor Network routing protocols are simple and this is a big reason that they are prone to network layer attacks.

3.1 Spoofed, Altered, or Replayed Routing Information

In this type of attack the information can be altered, spoofed or replayed by an attacker which is going to exchange between sensor nodes. The attacker can remove or add some extra nodes in the network which can change the route of the existing nodes. [11]

3.2 Selective Forwarding

Generally in multihop network, nodes forward the packets that they received from other nodes to destination but it cannot happen in some cases, if an adversary present in a network or blackhole it will not forward the packets, drop them in midway or selectively forward the packets. [12]

3.3 Sybil Attack

The task which has to be performed is divided into subparts and distributed among sensor nodes which can also lead to redundancy of information. During this an adversary can appears in a multiple identities in a network by replicating legitimate nodes present in a network. It forges the identities of more than one legitimate node which leads to Sybil attack in a network. It destroys security, integrity and resource utilization of nodes. Sybil attack mostly performed to attack distributed storage, routing mechanism, allocation of resources, voting system of nodes. Detection of Sybil attack is very difficult in a network. Radio resource testing method can be used to detect Sybil nodes presence in a network. [13]

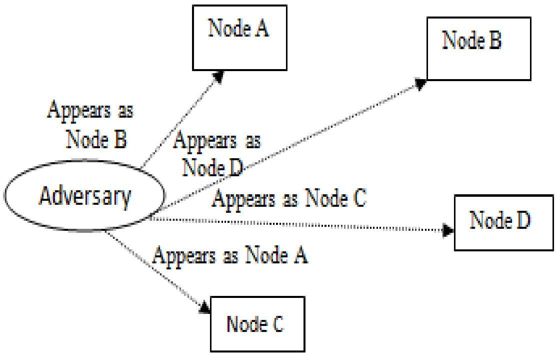


Fig. 3. Sybil Attack

3.4 Denial of service

In this type of attack the victim node is unable to access resources that are provided to it because they are exhausted by sending unwanted packets to the node so the legitimate nodes are unable to use resources in a network that are allocated to them. In this, base station cannot communicate with any other node and completely become useless because of the unwanted traffic in a network. This attack is different for different layers in a network. Jamming and tampering of information can be done at physical layer; at link layer collision can be done, at network layer neglecting or misdirection for the information, at transport layer malicious flooding of unwanted packets to the node is a DoS type of attack. There are some mechanisms present to prevent DoS are Authentication, identification of traffic, or payment for network resources. [14]

3.5 Sinkhole/Blackhole attack

In this type of attack blackhole node redirects all the traffic in the network. It is a malicious node. An adversary listens to requests in a network and then targets those nodes which are of high quality and close to base station and inserts itself in a network between legitimate nodes. After that it advertises that the route that is through the compromised node is the most trustworthy route in the network, As a result it can formulate or drop the packets those take compromised node for the packet forwarding. [15, 16]

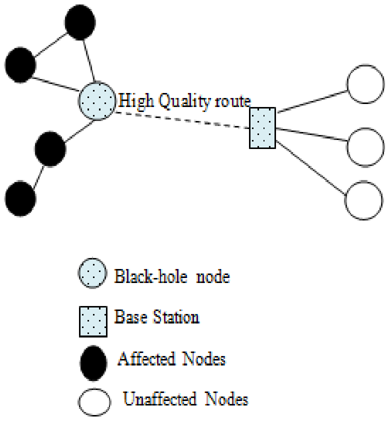


Fig. 4. Sinkhole/Blackhole Attack

3.6 Wormhole attack

In wormhole attack an attacker establishes its own link in the network. The attacker link is called as wormhole link in the network. When a sensor node broadcast a message in a network an attacker records all the packets and sends those packets to different location. The wormhole attack is very difficult to detect because it does not need any compromised node for attack and it can be perform at the initial phase of the communication, when sensor nodes are going to start searching for their neighboring nodes. [15, 16]

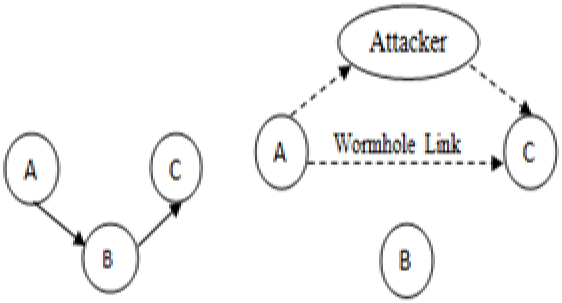


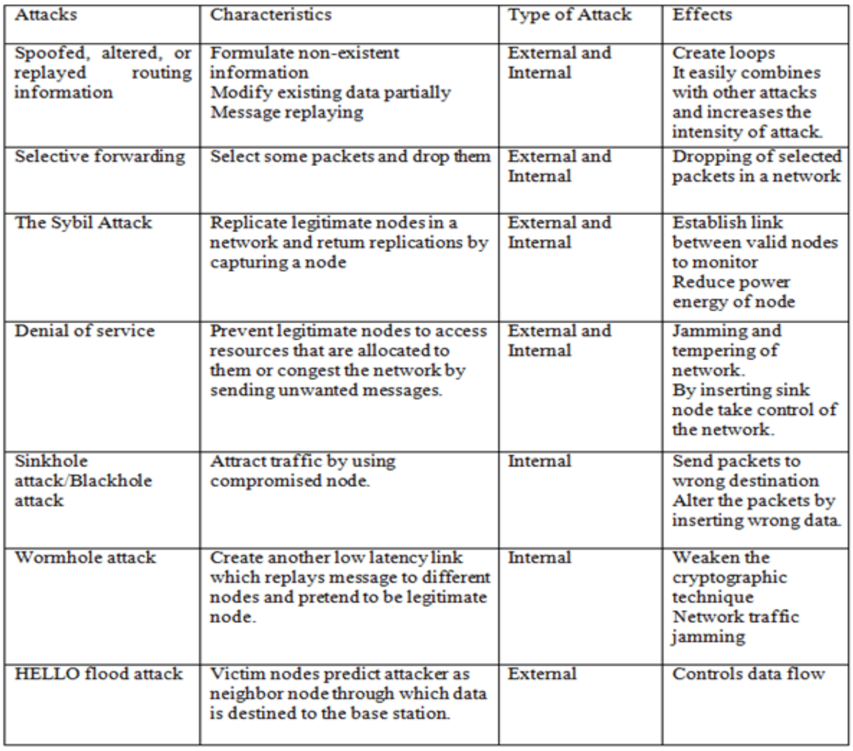
Fig. 5. Wormhole Attack

The figure shows the wormhole attack. In this node A broadcasts a message an attacker receives the message and broadcasts this message to its neighbor nodes. The nodes which receive this message believe that they are in the range of node A and mark the node as a parent node. Whether a node C is multihop but an attacker will convince the node that A is single hop away from it, therefore it will create wormhole attack.

3.7 HELLO Flood Attack

HELLO packets are used to broadcast the message to the neighbor nodes to tell the presence of the node in the network. Broadcasting a HELLO message is prone the HELLO flood attack. When a node in a network receives HELLO packet from the compromised node the node predicts that the node is present in the network and are in contact with each other in a radio range but the adversary which is far away from the network has a very strong transmitter so that it can reach to every node present in the network. Now adversary can control the sensor nodes completely. An adversary starts rebroadcasting overhead packets to every node in a network, after getting flooded by the messages when a node realizes that it got link to the adversary node, it left with very few options as every neighbor node is already in communication with an adversary node. It is an attack which can be external or internal for the network [15, 16].

Table.1. Attacks in Wireless Sensor Networks



Attacks	Characteristics	Type of Attack	Effects
Spoofed, altered, or replayed routing information	Formulate non-existent information Modify existing data partially Message replaying	External and Internal	Create loops It easily combines with other attacks and increases the intensity of attack.
Selective forwarding	Select some packets and drop them	External and Internal	Dropping of selected packets in a network
The Sybil Attack	Replicate legitimate nodes in a network and return replications by capturing a node	External and Internal	Establish link between valid nodes to monitor Reduce power energy of node
Denial of service	Prevent legitimate nodes to access resources that are allocated to them or congest the network by sending unwanted messages.	External and Internal	Jamming and tempering of network. By inserting sink node take control of the network.
Sinkhole attack/Blackhole attack	Attract traffic by using compromised node.	Internal	Send packets to wrong destination Alter the packets by inserting wrong data.
Wormhole attack	Create another low latency link which replays message to different nodes and pretend to be legitimate node.	Internal	Weaken the cryptographic technique Network traffic jamming
HELLO flood attack	Victim nodes predict attacker as neighbor node through which data is destined to the base station.	External	Controls data flow

IV. Security Mechanisms

Some of existing security mechanisms for sensor networks is: [17]

4.1 Security Primitives

Confidentiality, integrity and authentication can be provided with the help of security primitives. The security primitives can be Symmetric Key Cryptography technique, Public key cryptography, Hash Functions, or via using Message Authentication code technique.

4.2 Key Management and Secure Channels

Key management systems are used to create, distribute and maintain the secret keys in the network in order to build secure channels for the communication in the sensor networks.

4.3 Self-Healing and Self-Management Protocols

Self- healing mechanism detects the intruder presence and the trust of the system. Self management provides information whether the node is present in the region or not to the protocols.

4.4 Privacy and anonymity

The main threat for privacy mainly depends upon content, location and identity of elements of network.

4.5 Software-based Protection and Testing

Some software is implemented to differentiate between the adversary nodes and the valid nodes in the network which are present remotely by using remote attestation or radio fingerprinting of the nodes.

V. Defense Mechanisms for Reputation

There are different defense mechanisms for Reputation systems, which are discussed over here [18]

5.1 Preventing multiple identities (Sybil attacks)

There can be two types of solution which can deal with these type of attacks centralized and decentralized. In a centralized approach the uniqueness of the entity is verified via central authority. While in a decentralized technique as no central authority is present, so some other type of solutions can be used to prevent Sybil attack like a unique identity can be provided to the node, a network can co-ordinate to detect nodes with multiple identities, or a reputation for a particular node can be generated from the trustworthy sources present in a network.

5.2 Mitigating Spreading of False Rumors

An adversary can spread false reputations in a network but to avoid this there are two methods, in first method pre-trusted entities can be used, the second can be use some statistical methods like Bayesian Method to construct an accurate feedback system which can judge false nodes on the basis of threshold value.

5.3 Preventing Short-Term Abuse of the System

To avoid the attackers by abusing the system, degrade the reputation rapidly and then they have to re-enter in the system with a new identity. One method is when new node starts it should start with low reputation and increase it slowly for some amount of time and in another approach for gaining reputation, node have to provide more services than they get in return for gaining a good reputation in a system.

5.4 Mitigating Denial of Service Attacks

DoS attack can be prevented by using randomization technique. In the randomization technique participants are selected randomly for the calculation and distribution of reputation values. This can decrease the effect of malicious nodes in a network.

VI. Trust

Trust mechanism is a security feature which was introduced to protect the system from compromised nodes and is able to build the self healing system in a network. On the basis of previously defined rules in a network, trust factor determines whether access to the network is possible or not. Trust can be subjective or objective, the subjective trust is known as a belief in a system and [19] objective trust can be depicted as reputation of a system.

6.1 Characteristics of Trust

There are different characteristics of trust which are defined below:

i. Subjective

Node's Subjective trust opinion is presented by belief trust opinion in a system. Belief of a system can be developed by past judgments, reputed views and the capacity of a system which can be judged by its fault tolerance capacity, adaptability to the environment, stability and timeliness of the system.

ii. Dynamic

It is not a stable entity it changes over time. Earlier the node was trustworthy but when it becomes compromised node by adversary then the trust value will be decline.

iii. Asymmetric

It is not mandatory that if node A trusts node B then B have to trust A, B can distrust Node A. So it is independent between both the sides.

6.2 Values of Trust

The trustworthiness of a network can be determined by using trust values. The range can be [-1, 0, 1]. The trust values can be divided into three parts according to preset values of trust. [20]

- High score: This score means network is safe and is the first choice to choose.
- Low score: This score means network is not safe to choose and this behavior can be considered as a pessimistic behavior in the network.
- Middle Score: At the initial stage all the participants have trust values in the network.

6.3 Trust Models with Classical Methodologies

The Trust models have been proposed by many researchers in the field of Trust and Reputation. This section will discuss several trust models with classical measurements.

6.3.1 Bayesian Trust Model

This model is used for the management of trust. It is mostly used model for the trust management. It works in two ways: [21, 22]

a) **Objective:** In this view only data is analyzed. Only statistical analysis performed.

b) **Subjective:** In this view decisions have been taken by taking into account the confidence level.

In general the trust of a system depends on the past behavior of a node in a network. In Bayesian theory the trust is computed by following complete procedure of trust evaluation. Bayesian theory uses previous probabilities of an event, later which can be used as a evidence to show the trustworthiness of a system. Therefore, Bayesian theory calculates more suitable trust values as compare to other techniques. It can be combined with other fields also.

6.3.2 Beta Distribution System

The beta distribution method is a density function. Beta distribution allows estimating the predictive probability. Predictive probability depends upon the past interactions whether they were successful or failures. It is indexed by two parameters α (alpha) and β (beta).In this method the reputation value was computed in a binary form: positive or negative value. The reputation value is computed using beta probability density function which is represent as an expected value of beta density functions. The reputation and trust model has been developed by Josang for electronic commerce which was based on Beta distribution method. The past interactions (h) can be summarized with principal (pj) by using beta parameters α and β where:

$\alpha = \#s(h) + 1$ (number of successful interactions) …(1)

$\beta = \#f(h) + 1$ (number of unsuccessful interactions) …(2)

The α and β representation helps to estimate predictive probability which gives the probability of success in next interactions with pj. [23]

6.3.3 Subjective Logic Trust Model

Subjective logic trust model has been extended from the theory which was proposed by Dampster-Shafer. The theory was used for analyzing a Bayesian network and developing trust network. Subjective logic defines trust by using subjective beliefs in a network between arbitrary nodes in a network. It represents a practical belief calculus which is used to calculate trust of a network. Subjective logic is denoted by $\omega^{A}_{x.} = (b, d, u, a)$ which is called as opinion, where A denotes the subject (belief owner) on the truth statement of x. b represents belief, d represents disbelief and u represents uncertainty. The sum total of b, d and u is equal to 1, i.e. $b+ d+ u=1$. If number of opinions is given they can be ordered on the basis of their priority which is decided by different rules defined below:

1. The opinion which has the greatest probability expectation has the greatest opinion.
2. The opinion which has least uncertainty has the greatest opinion.
3. The opinion which has the least base rate has the greatest opinion. [24]

6.3.4 Entropy Trust Model

Entropy works on the concept of uninformativeness which means uncertainty. It is stated by Caticha and Giffin that maximum entropy method has a special case of Bayesian theory and maximum entropy because both are compatible with each other. The method which was also based on Bayesian and entropy based trust values method was proposed [25]. The entropy based value can be defined as:

$T= \{1-H(p)$ for $0.5 \le p \le 1$
$T= \{H(p)-1$ for $0 \le p < 0.5$
T= T{subject: agent; action}
P=p{subject :agent; action}

$H(p)= -p\log_2(p)-(1-p)\log_2(1-p)$ …(3)
H is entropy function
The trust value is not linear proportional to probability that means more the uncertainty less variation in trust value is.

6.3.5 Fuzzy Trust Model

The trust is not clear; it is vague, uncertain in nature so it cannot take as a probability in a network. Fuzzy logic deals with reasoning which is derived from Fuzzy set theory. It is not precise it deals with approximation. As truth is uncertain because the facts that are present in a network are not clear so the policy can be forced to be fuzzy also. Earlier the Subject logic trust model calculates uncertainty but all uncertainty cannot be considered as probability. But fuzzy trust models provide some fuzzy rules which can handle the uncertainty of trust management. In fuzzy trust models control system problems are solved using IF- Then rules. The rules for fuzzy logic are as follows: [26]

1) Define the fuzzy sets and criteria for them.
2) Initialization of input variables values to the fuzzy engine.
3) For calculating output data the fuzzy rules will be applied.
4) After evaluation of results feedback will be provided to rules.

6.3.6 Game Theory Trust Model

This theory captures the situation mathematically in which one's success after taking decision depends upon the behavior of others. It is also called as trust game for two players. In adhoc networks selfish behavior of nodes is an issue which can lead to uncooperative behavior between nodes so to avoid this issue several scholars proposed game theory for trust management. According to Prisoner's the interactions between different nodes can be modeled as a game. So this can avoid the uncooperative behavior of nodes in a network. Like previously defined theories game theory also cannot predict the behavior of nodes. The condition of game theory is that it is bidirectional in behavior but in wireless sensor networks it is one way transmission so game theory is not able to solve trust problems in wireless sensor networks. [27, 28]

6.4 Categorization of Trust Models

Further trust models can be divided into two categories: Node Trust Models and Data Trust Models. On the basis of these models the communication takes place in the network.

6.4.1 Node Trust Models

In Node trust models the trust value can be calculated by using two methods centralized and distributed. In centralized base station calculates the trust values of sensor nodes but in distributed model sensor nodes itself calculates the value of trust. Different Node Trust Models are defined below:

6.4.1.1 Trust Computation method using Fuzzy Logic (TCFL)

Trust is an entity on the basis of which one node communicates with another by take in account the risks. It is binary decision which has been taken on the basis of balance between trust and risk. Fuzzy logic deals with if- then rules. The if– then rules can be applied on control systems, pattern recognition and in decision making. The degree of each sensor node has been calculated. This model is used to calculate the trust values for the path in a network using the trust value of node. The path with the maximum trust value is chosen for the communication. Fuzzy logic is used to quantize the uncertain data so can find the exact path from source to destination. The trust of a node is calculated by using two variables T and U. T defines trustworthiness and U defines untrustworthiness. The range of T and U lies between 0 and 1. The reputation of each sensor node resides at base station which it gets by past judgments. There are different values of reputation for each sensor node in a network that are:

1. Min: $T=\min(T_i, T_j)$, Min: $U=\min(U_i, U_j)$

2. Max: $T=max(T_i, T_j)$, Max: $U=max(U_i,U_j)$

Therefore, trust and untrust in a network can be calculated as:
$T= avg(T_{i,}T_j)/1-(avg(T_i,,U_j)+avg(T_j,U_i))$ …(4)
$U= avg(U_i,U_j)/1-((T_i,,U_j)+avg(T_j,U_i))$ …(5)
By using values of T and U, evaluation level of sensor network can be calculated as:
Evaluation Value = T/(T+U) …(6)
The advantage of this technique is that it is using fuzzy logic which can quantize the uncertain data. But it is using centralized technique which is not suitable in sensor networks. [29]

6.4.1.2 Reputation-based Framework for Sensor Networks (RFSN)

Reputation is a node's opinion towards other node's intentions in a network which can be judge on the basis of past behaviors of a node in a network. RFSN is a framework in which it maintains the reputation for every sensor node in a network. In this framework the trustworthiness of a node is evaluated on the basis of its reputation in a network. At the time of communication, a node team up with those nodes that has more reputation. RFSN works in a distributed manner at the middleware of every sensor node. As it works in a distributed manner so there is no central authority for storing reputation in a network. Therefore, every sensor node stores reputation of every other node in a network. In RFSN the computation of trust depends on Watchdog mechanism. The nodes use watchdog mechanism for observing other nodes' actions in a network. The nodes are classified into two categories: cooperative and uncooperative. The nodes which are cooperative are more trustworthy. Trust is a neighbor nodes' belief for a sensor node in a network. Trust is updated according to age of a node. More the age, More the trustworthiness. The trust is precise and concise without any failure. But it is unable to make the system robust as it works only on node's reputation. [30]

6.4.1.3 Parameterized and Localized trust management Scheme (PLUS)

PLUS model is used in low cost sensor nodes. The large amount of information that is present can be easily quantify, visualize and exploit by using parameterization. Decision making parameters are easy to adapt because they consume less memory space as compare to lengthy codes. PLUS model uses personal references and recommendation for establishing trust in sensor nodes. Sensor nodes should be able to evaluate its local sites in terms of security, identification of failed neighbors and can take decisions intelligently while residing in a network. Sensor node Personal reference is calculated on nodes' availability and ratio of correct packets. Judge is a node which performs evaluation, the node which is judged by judge is known as Suspect and the node which keeps the trust value of the suspect for giving opinions periodically to judge is known as Jury. In distributed trust model there are two salient features: recommendation based trust and trust based recommendation. The judge who wants complete trustworthiness of the suspect requires personal reference and the reference which is recommendation based trust. Direct interaction or observed behavior of suspect gives the personal reference but recommendations will be taken by the juries in the network. Trust based recommendation completed by taking into account the trustworthiness of juries against malicious use. It can efficiently detect the malicious nodes in a network. But at the time of congested network it slows down because the trust convergence time is very high. [31]

6.4.1.4 Node Behavioral strategies Banding belief theory of the Trust Evaluation algorithm(NBBTE)

It calculates trust value on the basis of various trust factors which depend on interactions between neighbor nodes and combine it with the security level of network parallel with respect to time. Then it applies fuzzy set theory on the trust value to measure how much it belongs to the trust degree. After considering recommendations of neighbor nodes, D-S evidence theory will be used to obtain integrate trust values. The trust evaluation depends on a subject which makes observation on an object with third party recommendations. The trust value of object is obtained by subject directly and indirectly. The quantitative and qualitative analysis of factors should make which may affect the trustworthiness of node. The disadvantage of this trust model is that it needs high power batteries because it needs excess energy and time for communication with neighbors in a network. [32]

6.4.1.5 Agent based Trust model is proposed in WSNs (ATSN)

Agent based trust model works on watchdog mechanism and it runs at the middleware of the node. The watchdog mechanism is used to monitor the node's behavior within its radio range by using distributed method. In this method agent node maintains trust tables about a subset of these nodes. In this technique every node follows watchdog technique so they maintain trust table for other nodes. Agent nodes are used to monitor the behavior of nodes. The nodes which lie in the radio range of agent nodes are monitored in promiscuous mode. In this mode agent nodes monitors the nodes and classifies their actions. Then categorize them as good or bad nodes. Agent nodes have some modules which carry out specific function related to data and classified it as cooperative or uncooperative behavior. The watchdog mechanism completes its work in three phases: 1) Data collection 2) Data check 3) State count. In data collection the behavior of nodes in a radio range has been recorded in a fixed time. In Data check the collected data used as input data in different modules. In State count phase the node behavior will be considered as good or bad. This is the energy efficient technique and detects different attacks like bad mouthing attack but the trustworthiness of a network relies on Agent nodes, if any malicious node behaves as agent node then it will compromise the trustworthiness of a network. [33]

6.4.1.6 Task-based Trust framework for Sensor Networks (TTSN)

Trust for a sensor node calculated on the basis of reputation of different tasks. The reputation of different tasks of neighbor nodes is maintained by sensor node and this reputation is used to calculate the trustworthiness of nodes. It has two entities (i) Task (ii) Trust Manager Module which is used to build trust. Sensor nodes have a number of trust values. Trust is calculated by task in a network which makes it a generic approach to be applied on different sensor networks. But it doesn't use any recommendation or past observations for taking decisions. All the decisions taken are totally instantaneous. [34]

6.4.2 Data Trust Models

The trustworthiness of sensor nodes is not sufficient. The information can also be forged, tampered, eavesdrop during transmission. So it is also important to evaluate trust value for data.

6.4.2.1 DFDI

This trust model distinguishes forged data of illegal nodes from the innocent data of legitimate nodes. The area consists of sensor nodes divide into logical grids. A unique identity is assigned to every grid. Now sensor nodes validate location of their neighbor nodes present in a same grid using ECHO protocol. The nodes' own results will be considered to check the trustworthiness of its neighbor nodes' sensed data. Weighted summation of consistent value of sensing data, communication ability, and remained lifetime of node is used to calculate the trust. Finally, aggregated results send to sink node. It can detect compromised nodes and inconsistent data from malicious nodes but ECHO protocol consumes more energy. [35]

6.4.2.2 DFR

In Determining Faulty Readings (DFR) both arbitrary and noisy readings are considered as faulty readings. The correlation network is built by finding similar readings of two sensor nodes. Correlation network is represented as graph G= (V,E) where V represents sensor nodes and E represents correlation between two sensor nodes. Reading similarity between two nodes is shown by edge; if they have similarity then they are connected by an edge. The sensor nodes are ranked by Markov Chain in the network, Markov Chain is a mechanism which rates nodes by Sensor Ranks in terms of the correlation with other nodes. The trustworthiness of node is represented by Sensor Rank. Sensor Rank approach is more efficient than other techniques in term of determining faulty readings. Sensor rank gives precise trust computation but it is exposed to collusion attacks. [36]

6.4.2.3 MDLC

Mechanism based on Data Life Cycle is used to calculate the trustworthiness of sensor data on the basis of states of sensor data. There are three states: raw data, routed data and processed data. The data is raw which is sensed by sensor node until it has been routed or processed. When it is send to another node it will be considered as routed data. Data is processed when it is filtered or fused. The subjective logic is used to calculate the trustworthiness of raw data, routed data and processed data. It is unable to judge malicious attacks. [37]

6.4.2.4 TMCDE

In this Trust Model based on Communication trust, Energy Trust and DATA Trust, communication trust which is relationship value between two cooperation nodes is calculated on the basis of successful transactions rate. Energy trust refers to the power energy of node whether it is able to complete data processing tasks and novel communications in a network. Data trust reviews trust on the basis of fault tolerance and data consistency. It is unable to update the trust values. [38]

VII. Conclusion

WSN is an emerging technique and beneficial in many applications as they don't need humans to operate it. Sensor networks work in isolated and open areas therefore they are prone to security attacks. In this paper, we discussed applications of Wireless Sensor Networks, Security Threats on sensor networks and various existing security techniques against threats. Different defense mechanisms for Reputation in a system have been discussed. Compromised nodes were very difficult to detect in a network. Therefore different trust models have been proposed by researchers which have been discussed in this paper.

References

[1]. Culler, D. E and Hong,W., Wireless Sensor Networks, *Communication of the ACM, Vol. 47, No. 6*, June 2004, pp. 30-33.

[2]. Dai, S, Jing, X, and Li, L, Research and analysis on routing protocols for wireless sensor networks, *Proc. International Conference on Communications, Circuits and Systems, Volume 1*, 27-30 May, 2005, pp. 407-411

[3]. Shah, R.C. and Rabaey, J.M.. Energy aware routing for low energy ad hoc sensor networks. *Wireless Communications and Networking Conference, 2002. WCNC2002. 2002 IEEE* ,Vol. 1, pp. 350-355, 2002, March. IEEE.

[4]. Meesookho, C., Narayanan, S., and Raghavendra, C. S., Collaborative classification applications in sensor networks. *Sensor Array and Multichannel Signal Processing Workshop Proceedings, 2002*, 2002, August, pp. 370-374. IEEE.

[5]. Kintner-Meyer, Michael, and Michael R. Brambley, Pros & cons of wireless. *ASHRAE journal 44.11*, 2002, pp. 54-56.

[6]. Mainwaring, A., Culler, D., Polastre, J., Szewczyk, R., and Anderson, J., Wireless sensor networks for habitat monitoring, *Proceedings of the 1st ACM international workshop on Wireless sensor networks and applications*, 2002, September, pp. 88-97, ACM.

[7]. Biagioni, Edoardo S., and K. W. Bridges, The application of remote sensor technology to assist the recovery of rare and endangered species, *International Journal of High Performance Computing Applications 16.3*, 2002, pp. 315-324.

[8]. Arampatzis, Th, John Lygeros, and S. Manesis, A survey of applications of wireless sensors and wireless sensor networks, *Intelligent Control, 2005, Proceedings of the 2005 IEEE International Symposium on Mediterrean Conference on Control and Automation*, 2005, IEEE.

[9]. Sibley, Gabriel T., Mohammad H. Rahimi, and Gaurav S. Sukhatme, Robomote: A tiny mobile robot platform for large-scale ad-hoc sensor networks. *Robotics and Automation,2002. Proceedings. ICRA'02,IEEE International Conference on*. Vol. 2.,2002, IEEE.

[10]. Dantu, K., Rahimi, M., Shah, H., Babel, S., Dhariwal, A., and Sukhatme, G. S. Robomote: enabling mobility in sensor networks. In*Proceedings of the 4th international symposium on Information processing in sensor networks*, 2005, April, p. 55, IEEE Press

[11]. Villalba, J., and Lleida, E. , Speaker verification performance degradation against spoofing and tampering attacks. In *FALA workshop* , 2010, pp. 131-134.

[12]. Yu, B., and Xiao, B., Detecting selective forwarding attacks in wireless sensor networks, *Parallel and Distributed Processing Symposium, 2006. IPDPS 2006. 20th International* , 2006, April, pp. 8-pp, IEEE.

[13]. Douceur, J. R., The sybil attack. *Peer-to-peer Systems* , Springer Berlin Heidelberg ,2002, pp. 251-260.

[14]. Blackert, W. J., Gregg, D. M., Castner, A. K., Kyle, E. M., Hom, R. L., and Jokerst, R. M., Analyzing interaction between distributed denial of service attacks and mitigation technologies. *DARPA information survivability conference and exposition, 2003. Proceedings* , 2003, April Vol. 1, pp. 26-36, IEEE.

[15]. Pathan, A. S. K., Lee, H. W., and Hong, C. S., Security in wireless sensor networks: issues and challenges, *Advanced Communication Technology, 2006. ICACT 2006. The 8th International Conference*, 2006, February ,Vol. 2, pp. 6-pp, IEEE.

[16]. Karlof, Chris, and David Wagner., Secure routing in wireless sensor networks: Attacks and countermeasures, *Ad hoc networks* 1.2 ,2003, pp.293-315.

[17]. Lopez, Javier, Rodrigo Roman, and Cristina Alcaraz., Analysis of security threats, requirements, technologies and standards in wireless sensor networks, *Foundations of Security Analysis and Design V.* Springer Berlin Heidelberg, 2009, pp. 289-338.

[18]. Hoffman, K., Zage, D., and Nita-Rotaru, C., A survey of attack and defense techniques for reputation systems, *ACM Computing Surveys (CSUR), 42*(1), 1, 2009

[19]. Momani, M., Challa, S., and Alhmouz, R., Can we trust trusted nodes in wireless sensor networks? , *Computer and Communication Engineering, 2008. ICCCE 2008. International Conference on* pp. 1227-1232, 2008, May. IEEE.

[20]. Jøsang, Audun, Roslan Ismail, and Colin Boyd., A survey of trust and reputation systems for online service provision, *Decision support systems*43, *no. 2* (2007): 618-644.

[21]. Sun, Y. L., Han, Z., Yu, W., and Liu, K. R., A Trust Evaluation Framework in Distributed Networks: Vulnerability Analysis and Defense Against Attacks. In *INFOCOM* (Vol. 2006), 2006, April, pp. 1-13.

[22]. Nielsen, M., Krukow, K., and Sassone, V., A bayesian model for event-based trust, *Electronic Notes in Theoretical Computer Science, 172*, , 2007, pp. 499-521.

[23]. ElSalamouny, Ehab, Karl Tikjøb Krukow, and Vladimiro Sassone, An analysis of the exponential decay principle in probabilistic trust models, *Theoretical computer science 410, no. 41* (2009): 4067-4084.

[24]. Jøsang, A., Hayward, R., and Pope, S.,Trust network analysis with subjective logic, *Proceedings of the 29th Australasian Computer Science Conference-Volume 48*. Australian Computer Society, Inc, 2006, January, pp. 85-94.

[25]. Sun, Y. L., Han, Z., Yu, W., and Liu, K. R., A Trust Evaluation Framework in Distributed Networks: Vulnerability Analysis and Defense Against Attacks. In *INFOCOM* (Vol. 2006), 2006, April, pp. 1-13.

[26]. Boukerche, A., and Ren, Y., A trust-based security system for ubiquitous and pervasive computing environments, *Computer Communications, 31*(18), 2008, pp. 4343-4351.

[27]. Jaramillo, J. J., and Srikant, R., DARWIN: distributed and adaptive reputation mechanism for wireless ad-hoc networks. In *Proceedings of the 13th annual ACM international conference on Mobile computing and networking* , 2007, September, ACM, pp. 87-98.

[28]. Papaioannou, T. G., and Stamoulis, G. D., Achieving honest ratings with reputation-based fines in electronic markets. In *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE*, 2008, April, IEEE.

[29]. Kim, Tae Kyung, and Hee Suk Seo., A trust model using fuzzy logic in wireless sensor network, *World academy of science, engineering and technology 42.6* (2008): 63-66.

[30]. Ganeriwal, Saurabh, Laura K. Balzano, and Mani B. Srivastava, Reputation-based framework for high integrity sensor networks, *ACM Transactions on Sensor Networks (TOSN)* 4.3 (2008): 15.

[31]. Yao, Z., Kim, D., and Doh, Y., PLUS: Parameterized and localized trust management scheme for sensor networks security. In *Mobile Adhoc and Sensor Systems (MASS), 2006 IEEE International Conference on* 2006, pp. 437-446. October, IEEE.

[32]. Feng, R., Xu, X., Zhou, X., and Wan, J., A trust evaluation algorithm for wireless sensor networks based on node behaviors and ds evidence theory.*Sensors, 11*(2), 2011, 1345-1360.

[33]. Chen, H., Wu, H., Zhou, X., and Gao, C., Agent-based trust model in wireless sensor networks. In *Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, 2007. SNPD 2007, Eighth ACIS International Conference on* (Vol. 3), 2007, pp. 119-124 July, IEEE.

[34]. Chen, Haiguang, Task-based trust management for wireless sensor networks. *International Journal of Security and its applications* 3.2 (2009): 21-26.

[35]. Hur, J., Lee, Y., Yoon, H., Choi, D., and Jin, S., Trust evaluation model for wireless sensor networks. In *Advanced Communication Technology, 2005, ICACT 2005, The 7th International Conference on* (Vol. 1), 2005, pp. 491-496, IEEE.

[36]. Xiao, X. Y., Peng, W. C., Hung, C. C., and Lee, W. C., Using sensor ranks for in-network detection of faulty readings in wireless sensor networks, In *Proceedings of the 6th ACM international workshop on Data engineering for wireless and mobile access* , (2007, June), pp. 1-8, ACM.

[37]. Gomez, L., Laube, A., and Sorniotti, A., Trustworthiness assessment of wireless sensor data for business applications, In *Advanced Information Networking and Applications, 2009. AINA'09. International Conference* , 2009 May, pp. 355-362, , IEEE

[38]. Hui-Hui, D., Ya-Jun, G., Zhong-Qiang, Y., and Hao, C., A wireless sensor networks based on multi-angle trust of node. In *Information Technology and Applications, 2009. IFITA'09. International Forum on* (Vol. 1), 2009, May, pp. 28-31. IEEE.